AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF CLAIMS

1. (Currently Amended)   A high reliability computer system, said system comprising:

a first processing engine (PE);

a first memory accessible by said first PE, containing initialization information for said first PE;

a second PE;

a second memory accessible by said second PE, containing initialization information for said second PE;

a third memory accessible by said first PE, said third memory having a location for storing an enable password for said first PE, the enable password protecting access to a privileged mode and execution of privileged mode commands;

a fourth memory accessible by said second PE;

circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE; and

a password passer writing said enable password of said first PE to the fourth memory accessible by said second PE.

2. (Original)   A high reliability computer system according to claim 1, wherein said password passer writes said enable password of said first PE to said fourth memory at the initialization of the system.

3. (Original)   A high reliability computer system according to claim 1, wherein said password passer writes said enable password of said first PE to said fourth memory every time said enable password of said first PE is changed.

4. (Original)   A high reliability computer system according to claim 1, wherein said password passer writes said enable password of said first PE to said fourth memory in response to a command from said second PE.

5. (Original)   A high reliability computer system according to claim 1, wherein password passer reads said enable password of said first PE from said first memory and writes said enable password to said fourth memory.

8
6. (Currently Amended)   A high reliability computer system, said system comprising:

a first PE;

a first memory accessible by said first PE, containing initialization information for said first PE;

a second PE;

a second memory accessible by said second PE, containing initialization

information for said second PE;

circuitry for automatically switching control of said system from said first PE to

said second PE upon detection of a failure of said first PE;

a password memory accessible by said first and second PEs, having a location for

storing an enable password for the system, the enable password protecting access to a

privileged mode and execution of privileged mode commands; and

a password keeper for maintaining said enable password in said password

memory for said first and second PEs.

9
7.(Original)   A high reliability computer system according to claim 8, wherein said

password keeper reads said enable password from said first memory and writes said

enable password to said password memory at the initialization of the system.

10
8.(Original)   A high reliability computer system according to claim 8, wherein said

initialization information for said first PE includes instructions for said password keeper

to write said enable password to said password memory.

11
9.(Original)   A high reliability computer system according to claim 8, wherein said

initialization information for said second PE includes instructions for said password

keeper to write said enable password to said password memory.

12

10. (Original)   A high reliability computer system according to claim 6, wherein said password keeper writes said enable password to said password memory every time said enable password is changed.

13

11. (Original)   A high reliability computer system according to claim 6, wherein said password keeper passes said enable password maintained in said password memory to either one of said first and second PEs in response to a request therefrom.

16

12. (Currently Amended)   A network system for providing password protection for a high reliability computer system, on a data communications network including a password server having a database for maintaining an enable password for said high reliability computer system, said password server being coupled via an information bus to said high reliability computer system, said system comprising:

a first PE;

a first memory accessible by said first PE, containing initialization information for said first PE;

a second PE;

a second memory accessible by said second PE, containing initialization information for said second PE;

circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE; and

an interface capable of communicating with the password server over the information bus, said interface obtaining an enable password from the password

server in response to a request from either one of said first and second PEs, the

enable password protecting access to a privileged mode and execution of

privileged mode commands.

17

16

13. (Original)   A network system according to claim 12, wherein said second PE

authenticates incoming users by requesting authentication from said password server.

18

16

14. (Original)   A network system according to claim 12, wherein said first PE obtains

said enable password from said password server via said interface at the initialization of

the system.

19

16

15. (Original)   A network system according to claim 12, wherein said initialization

information for said first PE includes instructions to access and obtain said enable

password from said password server.

22

16. (Currently Amended)   A system for providing password protection for a high

reliability computer system on a data communications network including a password

server having a database for maintaining an enable password for said high reliability

computer system, said password server being coupled via an information bus to said high

reliability computer system, said system comprising:

a first PE;

a first memory accessible by said first PE, containing initialization

information for said first PE;

a first interface for said first PE, said first interface capable of communicating user authentication requests and responses with the password server over the information bus, said first interface obtaining an enable password from the password server in response to a request from said first PE, the enable password protecting access to a privileged mode and execution of privileged mode commands;

a second PE;

a second memory accessible by said second PE, containing initialization information for said second PE;

a second interface for said second PE, said second interface capable of communicating user authentication requests and responses with the password server over the information bus, said second interface obtaining said enable password from the password server in response to a request from said second PE; and

circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE.

25

17. (Currently Amended)   A method for operating a high reliability computer system, said system including a first PE, a first memory accessible by said first PE, said first memory containing initialization information for said first PE and having a location for storing an enable password for said first PE, a second PE, and a second memory accessible by said second PE, said second memory containing initialization information for said second PE, said method comprising:

writing said enable password of said first PE to a third memory accessible by said

second PE, said enable password protecting access to a privileged mode and execution of

privileged mode commands; and

automatically switching control of said system from said first PE to said second

PE upon detection of a failure of said first PE.

26
18.(Original)   A method according to claim 17, wherein said writing of said enable

password of said first PE to said third memory is performed at the initialization of the

system.

27
19.(Original)   A method according to claim 17, wherein said writing of said enable

password of said first PE to said third memory is performed every time said enable

password of said first PE is changed.

28
20. (Original)   A method according to claim 17, wherein said writing of said enable

password of said first PE to said third memory is performed in response to a command

from said second PE.

31
21. (Currently Amended)   A method for operating a high reliability computer system,

said system including a first PE, a first memory accessible by said first PE, said first

memory containing initialization information for said first PE, a second PE, and a second

memory accessible by said second PE, said second memory containing initialization

information for said second PE, said method comprising:

providing a password memory accessible by said first and second PEs, having a

location for storing an enable password, said enable password protecting access to a

privileged mode and execution of privileged mode commands;

maintaining said enable password for said first and second PEs in said password

memory; and

automatically switching control of said system from said first PE to said second

PE upon detection of a failure of said first PE.

32

31

~~22.~~ (Original) A method according to claim ~~21,~~ wherein said maintaining includes:

reading said enable password from said first memory and writing said enable

password to said password memory at the initialization of the system.

33

31

~~23.~~ (Original) A method according to claim ~~21,~~ wherein said maintaining includes:

writing said enable password to said password memory every time said enable

password is changed.

34

31

~~24.~~ (Original) A method according to claim ~~21,~~ wherein said maintaining includes:

writing said enable password to said password memory in response to a command

from said first PE.

35

31

~~25.~~ (Original) A method according to claim ~~21,~~ wherein said maintaining includes:

passing said enable password maintained in said password memory to either one

of said first and second PEs in response to a request therefrom.

38

26. (Currently Amended)   A method for providing password protection for a high

reliability computer system, said system including a first PE, a first memory accessible

by said first PE, said first memory containing initialization information for said first PE, a

second PE, a second memory accessible by said second PE, said second memory

containing initialization information for said second PE, and circuitry for automatically

switching control of said system from said first PE to said second PE upon detection of a

failure of said first PE, said method comprising:

sending an enable password for the high reliability computer system for storage in

a database of a server coupled to the high reliability computer system via an information

bus, the enable password protecting access to a privileged mode and execution of

privileged mode commands;

providing an interface capable of communicating with the password server over

the information bus; and

obtaining the enable password from the password server through the interface in

response to a request from either one of the first and second PEs.

41   40   38
27. (Original) A method according to claim 26, further comprising authenticating

incoming users by requesting authentication from the password server.

42

28. (Currently Amended)   A method for providing password protection for a high

reliability computer system, said system including a first PE, a first memory accessible

by said first PE, said first memory containing initialization information for said first PE, a

second PE, a second memory accessible by said second PE, said second memory

containing initialization information for said second PE, and circuitry for automatically

switching control of said system from said first PE to said second PE upon detection of a

failure of said first PE, said method comprising:

sending an enable password for the high reliability computer system for storage in

a database of a password server coupled to the high reliability computer system via an

information bus, the enable password protecting access to a privileged mode and

execution of privileged mode commands;

communicating user authentication requests and responses with the password

server over the information bus via a first interface and obtaining the enable password

from the password server for the first PE, the enable password protecting access to a

privileged mode and execution of privileged mode commands; and

communicating user authentication requests and responses with the password

server over the information bus via a second interface and obtaining the enable password

from the password server for said second PE.

45
29. (Currently Amended)   A program storage device readable by a machine, tangibly

embodying a program of instructions executable by the machine to perform method steps

for operating a high reliability computer system, said system including a first PE, a first

memory accessible by said first PE, said first memory containing initialization

information for said first PE and having a location for storing an enable password for said

first PE, a second PE, and a second memory accessible by said second PE, said second

memory containing initialization information for said second PE, said method steps

comprising:

writing said enable password of said first PE to a third memory accessible by said

second PE, said enable password protecting access to a privileged mode and execution of

privileged mode commands; and

automatically switching control of said system from said first PE to said second

PE upon detection of a failure of said first PE.

46
30. (Original) A program storage device according to claim 29, wherein said method step

of writing said enable password of said first PE to said third memory is performed at the

initialization of the system.

47
31. (Original) A program storage device according to claim 29, wherein said method step

of writing said enable password of said first PE to said third memory is performed every

time said enable password of said first PE is changed.

48
32. (Original) A program storage device according to claim 29, wherein said method step

of writing said enable password of said first PE to said third memory is performed in

response to a command from said second PE.

51
33. (Currently Amended)   A program storage device readable by a machine, tangibly

embodying a program of instructions executable by the machine to perform method steps

for operating a high reliability computer system, said system including a first PE, a first

memory accessible by said first PE, said first memory containing initialization

information for said first PE, a second PE, and a second memory accessible by said

second PE, said second memory containing initialization information for said second PE,

said method steps comprising:

providing a password memory accessible by said first and second PEs, having a

location for storing an enable password, said enable password protecting access to a

privileged mode and execution of privileged mode commands;

maintaining said enable password for said first and second PEs in said password

memory; and

automatically switching control of said system from said first PE to said second

PE upon detection of a failure of said first PE.

52.
34. (Original) A program storage device according to claim 51, wherein said method step

of maintaining includes:

· reading said enable password from said first memory and writing said enable

password to said password memory at the initialization of the system.

53
35. (Original) A program storage device according to claim 51, wherein said method step

of maintaining includes:

writing said enable password to said password memory every time said enable

password is changed.

54
36. (Original) A program storage device according to claim 33, wherein said method step of maintaining includes:

writing said enable password to said password memory in response to a command from said first PE.

55
37. (Original) A program storage device according to claim 33, wherein said method step of maintaining includes:

passing said enable password maintained in said password memory to either one of said first and second PEs in response to a request therefrom.

58
38. (Currently Amended)   A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for providing password protection for a high reliability computer system, said system including a first PE, a first memory accessible by said first PE, said first memory containing initialization information for said first PE, a second PE, a second memory accessible by said second PE, said second memory containing initialization information for said second PE, and circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE, said method steps comprising:

sending an enable password for the high reliability computer system for storage in a database of a password server coupled to the high reliability computer system via an information bus, the enable password protecting access to a privileged mode and execution of privileged mode commands on the high reliability computer system;

providing an interface capable of communicating with the password server over

the information bus; and

obtaining the enable password from the password server through the interface in

response to a request from either one of the first and second PEs.

59

58

39. (Original)   A program storage device according to claim 38, wherein said method

steps further comprises authenticating incoming users by requesting authentication from

the password server.

62

40. (Currently Amended)   A program storage device readable by a machine, tangibly

embodying a program of instructions executable by the machine to perform method steps

for providing password protection for a high reliability computer system, said system

including a first PE, a first memory accessible by said first PE, said first memory

containing initialization information for said first PE, a second PE, a second memory

accessible by said second PE, said second memory containing initialization information

for said second PE, and circuitry for automatically switching control of said system from

said first PE to said second PE upon detection of a failure of said first PE, said method

steps comprising:

sending an enable password for the high reliability computer system for storage in

a database of an authentication, authorization and accounting (AAA) server coupled to

the high reliability computer system via an information bus, the enable password

protecting access to a privileged mode and execution of privileged mode commands on

the high reliability computer system;

communicating user authentication requests and responses with the <u>AAA</u>
~~password~~ server over the information bus via a first interface <u>and obtaining the enable</u>
<u>password from the AAA server</u> for the first PE; and

communicating user authentication requests and responses with the <u>AAA</u>
~~password~~ server over the information bus via a second interface <u>and obtaining the enable</u>
<u>password from the AAA server</u> for the second PE.

65
~~41.~~(Currently Amended)   An apparatus for operating a high reliability computer
system, said system including a first PE, a first memory accessible by said first PE, said
first memory containing initialization information for said first PE and having a location
for storing an enable password for said first PE, a second PE, and a second memory
accessible by said second PE, said second memory containing initialization information
for said second PE, said <u>apparatus</u> ~~method~~ comprising:

means for writing said enable password of said first PE to a third memory
accessible by said second PE<u>, said enable password protecting access to a privileged</u>
<u>mode and execution of privileged mode commands</u>; and

means for automatically switching control of said system from said first PE to
said second PE upon detection of a failure of said first PE.

68
~~42.~~(Currently Amended)   An apparatus for operating a high reliability computer
system, said system including a first PE, a first memory accessible by said first PE, said
first memory containing initialization information for said first PE, a second PE, and a

second memory accessible by said second PE, said second memory containing

initialization information for said second PE, said <u>apparatus</u> ~~method~~ comprising:

means for providing said first and second PEs with access to an enable password,

<u>the enable password protecting access to a privileged mode and execution of privileged</u>

<u>mode commands</u>;

means for maintaining said enable password for said first and second PEs; and

means for automatically switching control of said system from said first PE to

said second PE upon detection of a failure of said first PE.

71

.~~43~~. (Currently Amended)   An apparatus for providing password protection for a high

reliability computer system, said system including a first PE, a first memory accessible

by said first PE, said first memory containing initialization information for said first PE, a

second PE, a second memory accessible by said second PE, said second memory

containing initialization information for said second PE, and circuitry for automatically

switching control of said system from said first PE to said second PE upon detection of a

failure of said first PE, said <u>apparatus</u> ~~method~~ comprising:

means for sending an enable password for the high reliability computer system for

storage in a database of a <u>password</u> server coupled to the high reliability computer system

via an information bus, <u>the enable password protecting access to a privileged mode and</u>

<u>execution of privileged mode commands on the high reliability computer system</u>; and

means for communicating with the password server over the information bus and

obtaining the enable password from the password server in response to a request from

either one of the first and second PEs.

74

44. (Currently Amended)   An apparatus for providing password protection for a high

reliability computer system, said system including a first PE, a first memory accessible

by said first PE, said first memory containing initialization information for said first PE, a

second PE, a second memory accessible by said second PE, said second memory

containing initialization information for said second PE, and circuitry for automatically

switching control of said system from said first PE to said second PE upon detection of a

failure of said first PE, said apparatus method comprising:

means for sending an enable password for the high reliability computer system for

storage in a database of a password server coupled to the high reliability computer system

via an information bus, the enable password protecting access to a privileged mode and

execution of privileged mode commands;

means for communicating user authentication requests and responses with the

password server over the information bus via a first interface and obtaining the enable

password from the password server for the first PE; and

means for communicating user authentication requests and responses with the

password server over the information bus via a second interface and obtaining the enable

password from the password server for the second PE.

65. (New)   A high reliability computer system according to claim 1, wherein said

system is a network device.

47.
46. (New)   A high reliability computer system according to claim 6, wherein said

network device is a router.

14
47. (New)   A high reliability computer system according to claim 8, wherein said

system is a network device.

15
48. (New)   A high reliability computer system according to claim 14, wherein said

network device is a router.

20
49. (New)   A network system according to claim 16, wherein the high reliability

computer system is a network device.

21
50. (New)   A network system according to claim 20, wherein said network device is a

router.

23
51. (New)   A system according to claim 22, wherein the high reliability computer

system is a network device.

24
52. (New)   A system according to claim 23, wherein said network device is a router.

29
53. (New)   A method according to claim 25, wherein the high reliability computer

system is a network device.

30

54. (New)   A method according to claim *53* ~~29~~, wherein said network device is a router.

36

36 *31*

55. (New)   A method according to claim ~~21~~ *31*, wherein the high reliability computer system is a network device.

37

36

56. (New)   A method according to claim ~~55~~ *36*, wherein said network device is a router.

39

38

57. (New)   A method according to claim ~~26~~ *38*, wherein the high reliability computer system is a network device.

40

39

58. (New)   A method according to claim ~~57~~ *39*, wherein said network device is a router.

43

42

59. (New)   A method according to claim ~~28~~ *42*, wherein the high reliability computer system is a network device.

44

43

60. (New)   A method according to claim ~~59~~ *43*, wherein said network device is a router.

49

45

61. (New)   A program storage device according to claim ~~29~~ *45*, wherein the high reliability computer system is a network device.

50

44

62. (New)   A program storage device according to claim ~~61~~ *44*, wherein said network device is a router.

56

63. (New)   A program storage device according to claim 33, wherein the high

reliability computer system is a network device.

57

64. (New)   A program storage device according to claim 63, wherein said network

device is a router.

60

65. (New)   A program storage device according to claim 38, wherein the high

reliability computer system is a network device.

61

66. (New)   A program storage device according to claim 65, wherein said network

device is a router.

63

67. (New)   A program storage device according to claim 40, wherein the high

reliability computer system is a network device.

64

68. (New)   A program storage device according to claim 67, wherein said network

device is a router.

66

69. (New)   An apparatus according to claim 41, wherein the high reliability computer

system is a network device.

67

70. (New)   An apparatus according to claim 69, wherein said network device is a

router.

69
71. (New)   An apparatus according to claim 42, wherein the high reliability computer

system is a network device.

70
72. (New)   An apparatus according to claim 71, wherein said network device is a

router.

72
73. (New)   An apparatus according to claim 43, wherein the high reliability computer

system is a network device.

73
74. (New)   An apparatus according to claim 73, wherein said network device is a

router.

74
75. (New)   An apparatus according to claim 44, wherein the high reliability computer

system is a network device.

76. (New)   An apparatus according to claim 75, wherein said network device is a

router.

77. (New)   A security system for providing password protection for a high reliability

network device on a data communications computer network, said security system

comprising:

a password server having a database for maintaining an enable password for the

high reliability network device, said password server being coupled via an information

bus to the high reliability network device; and

the high reliability network device, including:

a first processing engine (PE);

a first memory accessible by said first PE, containing initialization

information for said first PE;

a second PE;

a second memory accessible by said second PE, containing initialization

information for said second PE;

circuitry for automatically switching control of said system from said first

PE to said second PE upon detection of a failure of said first PE; and

an interface capable of communicating with said password server over the

information bus, said interface obtaining an enable password from said password

server in response to a request from either one of said first and second PEs, the

enable password protecting access to a privileged mode and execution of

privileged mode commands.

78. (New)   A security system according to claim 77, wherein said second PE

authenticates incoming users by requesting authentication from said password server.

79. (New)   A security system according to claim 77, wherein said first PE obtains

said enable password from said password server via said interface at the initialization of

the system.

80. (New)   A security system according to claim 77, wherein said initialization

information for said first PE includes instructions to access and obtain said enable

password from said password server.

81. (New)   A security system for providing password protection for a high reliability

network device on a data communications network, said security system comprising:

        a password server having a database for maintaining an enable password for the

high reliability network device, said password server being coupled via an information

bus to said high reliability network device; and

        the high reliability network device, including:

                a first PE;

                a first memory accessible by said first PE, containing initialization

        information for said first PE;

                a first interface for said first PE, said first interface capable of

        communicating user authentication requests and responses with the password

        server over the information bus, said first interface obtaining an enable password

        from the password server in response to a request from said first PE, the enable

        password protecting access to a privileged mode and execution of privileged

        mode commands;

a second PE;

a second memory accessible by said second PE, containing initialization information for said second PE;

a second interface for said second PE, said second interface capable of communicating user authentication requests and responses with the password server over the information bus, said second interface obtaining said enable password from the password server in response to a request from said second PE; and

circuitry for automatically switching control of said system from said first PE to said second PE upon detection of a failure of said first PE.

82. (New)   A high reliability network device, comprising:

a first processing engine (PE);

a first memory accessible by said first PE, containing initialization information for said first PE;

a first consol port coupled to said first PE via a bus, adapted to receive commands from a first consol;

a second PE;

a second memory accessible by said second PE, containing initialization information for said second PE;

a second consol port coupled to said second PE via the bus, adapted to receive commands from a second consol;

a third memory accessible by said first PE, said third memory having a location

for storing an enable password for said first PE, the enable password protecting access to

a privileged mode and execution of privileged mode commands;

a fourth memory accessible by said second PE;

circuitry for automatically switching control of said system from said first PE to

said second PE upon detection of a failure of said first PE; and

a password passer writing said enable password of said first PE to the fourth

memory accessible by said second PE.

83. (New)   A high reliability network device, comprising:

a first PE;

a first memory accessible by said first PE, containing initialization information for

said first PE;

a first consol port coupled to said first PE via a bus, adapted to receive commands

from a first consol;

a second PE;

a second memory accessible by said second PE, containing initialization

information for said second PE;

a second consol port coupled to said second PE via the bus, adapted to receive

commands from a second consol;

circuitry for automatically switching control of said system from said first PE to

said second PE upon detection of a failure of said first PE;

a password memory accessible by said first and second PEs, having a location for

storing an enable password for the system, the enable password protecting access to a

privileged mode and execution of privileged mode commands; and

a password keeper for maintaining said enable password in said password

memory for said first and second PEs.

84. (New)   A high reliability network device, comprising:

a first processing engine (PE);

a first memory accessible by said first PE, containing initialization information for

said first PE; and

a first consol port coupled to said first PE via a bus, adapted to receive commands

from a first consol;

a second PE;

a second memory accessible by said second PE, containing initialization

information for said second PE; and

a second consol port coupled to said second PE via the bus, adapted to receive

commands from a second consol;

circuitry for automatically switching control of said system from said first PE to

said second PE upon detection of a failure of said first PE; and

an interface coupled to said first and second PEs via the bus, said interface being

capable of communicating with a password server over an information bus, said interface

obtaining an enable password from the password server in response to a request from

either one of said first and second PEs, the enable password protecting access to a

privileged mode and execution of privileged mode commands.

85. (New)   A high reliability network device according to claim 84, wherein said

interface comprises:

a first interface dedicated to said first PE; and

a second interface dedicated to said second PE.